REMARKS

Claims 1-33 are currently pending in the subject application and are presently under consideration. Claims 1, 17 and 33 have been amended herein to further emphasize various novel features. A version of all claims is shown at pages 2-8 of this Reply.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-33 Under 35 U.S.C. §102(e)

Claims 1-33 stand rejected under 35 U.S.C. §102(e) as being anticipated by Shambroom (2001/0020274 A1). Withdrawal of this rejection is respectfully requested for at least the following reasons. Shambroom fails to teach or suggest each and every limitation as recited in the subject claims. Moreover, Shambroom is a continuation-in-part of Shambroom (US 6,198,824), yet virtually all of the material relied upon by the Examiner to make this rejection is new subject matter that is not granted the priority of the parents. In particular, the new subject matter disclosed in Shambroom not taught or suggested by the parents includes at least paragraphs 0104-0139 and FIGS. 8-11D.

> A single prior art reference anticipates a patent claim only if it expressly or inherently describes ***each and every limitation set forth in the patent claim***. *Trintec Industries, Inc., v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 U.S.P.Q.2D 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987) (emphasis added). ***The identical invention must be shown in as complete detail as is contained in the ... claim***. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

Applicants' claimed invention relates to controlling a client's access to remote resources by redirecting data packets from a client to an Access Control Web Server (ACWS). Specifically, a gateway can ***rewrite the destination IP address*** intended for a destination server with the IP address of the ACWS, and can transmit the ***entire*** packet to the ACWS. In particular, independent claim 1 (and similarly independent claim 17) recites, "***redirecting the entirety*** of each of the ***handshaking packets***". Additionally, independent claim 1 (and similarly

independent claims 17 and 33) recites, "***redirecting*** the content request packet ***in its entirety*** by ***rewriting the destination address in the packet IP header*** to route the packet to the access controlling web server" and "at the gateway controlling access of the client machine to the desired resource based on the ***response from the access controlling web server***".

Shambroom relates to providing secure remote operations over an insecure computer network between a client and a remote host. Specifically, Shambroom employs a Kerberos Server for principal authentication based upon the client's user name and password (*see* paragraph 0078) and, using this information, supplies a ticket-granting ticket and an encrypted session key (*see* para. 0081), and/or other information which is used to create Secure Socket Layers (SSL) for secure/encrypted communication. Once proper login has been accomplished, the client sends both credentials and remote command data to the gateway. (*See* paragraph 0108). The credentials are intended for the Kerberos Server, and the remote command data is intended for the remote host. The gateway ensures this is precisely what occurs, as the remote command client servlet 2400 (which resides on the gateway) separates the information from the client into two parts. The credentials get sent to the Kerberos server, where they are authenticated and then used to create an SSL between the gateway and the remote host. (*See* paragraphs 0109-0113). Secondly, the remote command data gets sent to the remote host over this SSL. (*See* paragraphs 0114-0115).

Accordingly, the initial handshake between the gateway and the remote host occurs **after** all communication with the Kerberos Server has completed. (*See* paragraph 0115). Once the handshake is requested, it is not redirected to the Kerberos Server (or anywhere else). Moreover, only a portion of the client data goes to the Kerberos Server, *i.e.*, the credentials, but not the remote command data or the handshake. Thus, Shambroom does not teach or suggest ***redirecting the entirety*** of each of the ***handshaking packets***, as recited in independent claims 1 and 17. As well, Shambroom does not teach or suggest ***redirecting*** the content request packet ***in its entirety*** by ***rewriting the destination address in the packet IP header***, as recited in independent claims 1, 17 and 33. In fact, Shambroom does not teach or suggest redirecting the handshakes or the content request (*e.g.*, the remote command data) at all, let alone doing so by rewriting the destination address in the packet IP header.

Rather, the data from the client that is intended for the remote host (*e.g.*, the remote command data such as messages or transactions), arrives the gateway and is sent to the remote

host, which is precisely where it was intended. Likewise, the data that does actually go to the Kerberos Server (*e.g.*, the credential cache) was never intended to go to the remote host, so, again, the gateway does not redirect any data, but instead send the data where the client intends. Moreover, the Kerberos server does not determine whether access to the remote host will be granted, but instead determines whether an *authenticated, secure* connection to the remote host can be created. The remote host determines if the client has access to the remote host and permission to execute the remote command based upon the ACL (*see* paragraph 0117). In contrast, the subject claims recite, "at the gateway controlling access of the client machine to the desired resource based on the ***response from the access controlling web server***. Accordingly, the gateway of Shambroom does not control (no ability to grant or deny) access to the remote host based upon a response from the Kerberos Server.

For at least the aforementioned reasons, Shambroom does not teach or suggest each and every feature of the claimed invention. Shambroom does not redirect packets intended for the remote host to the Kerberos Server, but instead sends credential information to the Kerberos server in order to create secure connections over which the information intended for the remote host is sent to the remote host without being redirected. Regardless, Shambroom does not teach or suggest rewriting the destination address in the packet IP header, and since the gateway of Shambroom separates the data sent from the client into portions, packets sent by the client cannot be redirected in their entirety. Furthermore, Shambroom does not teach or suggest controlling access to the remote host based upon a response from the Kerberos server. In view of the foregoing, this rejection of independent claims 1, 17 and 33, as well as all associated dependent claims, should be withdrawn.

CONCLUSION

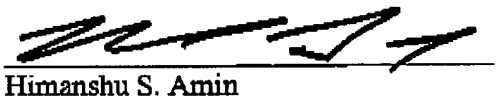
The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP1148US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN & TUROCY, LLP



Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731